Elektronische Gesundheitskarte und Telematikinfrastruktur

Informationsblatt Sicherheitsgutachten Signaturdienst

Version: 1.0.0
Stand: 04.05.2020

Zulassungsnehmer des Signaturdienstes müssen nicht alle Anteile des Signaturdienstes selbst betreiben. Anteile können von einem Betreiber (z.B. einer Krankenkasse) übernommen werden.

Der Zulassungsnehmer ist für die Umsetzung aller Anforderungen des Anbietertypsteckbriefs in allen Anteilen des Signaturdienstes verantwortlich. Dies beinhaltet auch die von einem beauftragten Betreiber betriebenen Anteile des Signaturdienstes.

Dieses Informationsblatt soll den Sicherheitsgutachtern des Signaturdienstes bei der Erstellung des Sicherheitsgutachtens in solchen verteilten Umsetzungsszenarien unterstützen.

Sicherheitsgutachter erstellen das Sicherheitsgutachten nach den üblichen Vorgaben der gematik. Darüber hinaus enthält die folgende Tabelle Aspekte, die im Falle des Signaturdienstes vom Sicherheitsgutachter im Sicherheitsgutachten zwingend zu dokumentieren sind. Der Zulassungsnehmer wird mit ZN bezeichnet, ein Betreiber mit BTR.

Abschnitt „Beschreibung des Prüfobjekts" Im Sicherheitsgutachten ist das Prüfobjekt zu beschreiben. Dies umfasst insbesondere die folgenden Aspekte.
Systemüberblick • In der Beschreibung sind alle Anteile des Signaturdienstes, die vom Sicherheitsgutachter geprüft wurden und die zum Zulassungsobjekt gehören, darzustellen. • Es muss ersichtlich sein, welche Anteile vom ZN selbst und welche ggf. von einem BTR betrieben werden. • Es ist insbesondere auch der User Helpdesk bzw. die Kontaktstelle für Anfragen von Nutzern bzgl. al.vi zu betrachten. Es ist darzustellen, wer diesen betreibt (der ZN selbst oder ein BTR). • Die angrenzenden Systeme, die nicht vom Sicherheitsgutachter geprüft werden, sind darzustellen. **Authentifizierungsverfahren** • Es sind die vom Signaturdienst angebotenen Authentifizierungsverfahren zu beschreiben. • Es ist für jedes Authentifizierungsverfahren darzustellen, wie das Sicherheitsniveau von „substanziell" (oder höher) erreicht wird. • Es ist darzustellen, ob das bzw. die vom Signaturdienst angebotene(n) Authentifizierungsverfahren Anforderungen an die Endgeräte der Versicherten verlangen (z.B. spezielle Hardware, sichere Speicherung von Authentifizierungsmerkmalen), auf denen die Clients zur Authentisierung am Signaturdienst ausgeführt werden. Falls ja, sind diese anzugeben. **Beantragungsprozess al.vi** • Es sind die Prozesse darzustellen, wie die Beantragung einer al.vi durch die Krankenkasse beim Signaturdienst erfolgt (Schnittstelle P_Create_Identity).

• Es sind die Maßnahmen darzustellen, die eine missbräuchliche Beantragung verhindern.
Dokumentation der Prüfergebnisse
• In der Dokumentation der Prüfergebnisse muss für jede Anforderung nachvollziehbar sein, ob sie vom ZN, vom BTR oder anteilmäßig von beiden umgesetzt wird. • Setzen sowohl ZN als auch BTR eine Anforderung um, ist darzustellen, welche Anteile jeweils vom ZN und welche vom BTR umgesetzt werden. • Es ist darzustellen, wie der ZN sicherstellt, dass alle Anforderungen des Anbietertypsteckbriefs, die sich auf Anteile des BTRs beziehen, auch vom BTR umgesetzt werden.
A_17336 - Signaturdienst - Sicherheitsniveau "substanziell" gemäß eIDAS-Verordnung **A_18172 - Signaturdienst - Authentifizierungsverfahren erfüllen TR-03107-1 für substanziell**
• Es ist darzustellen, welche Anteile des Signaturdienstes welchen Beitrag zur Umsetzung des Sicherheitsniveaus von „substanziell" umsetzen. • Es ist darzustellen, dass alle angebotenen Authentifizierungsverfahren die Anforderungen der TR-03107-1 erfüllen.
A_17864 - Signaturdienst - Anbieter des Signaturdienstes ist kein Anbieter eines ePA-Aktensystems
• Falls ein BTR, der Anteile des Signaturdienstes betreibt, gleichzeitig ein Anbieter eines ePA-Aktensystems ist, ist darzustellen, wie der in A_17864 geforderte Rollenausschluss sichergestellt wird.
A_18765 - Gemeinsame Kontaktstelle von Signaturdienst und ePA-Aktensystem
• Falls eine Kontaktstelle für Nutzeranfragen bzgl. al.vi angeboten wird, ist auch diese vom Sicherheitsgutachter zu prüfen. Dies gilt auch für den Fall, dass die Kontaktstelle nicht vom ZN selbst, sondern von einem BTR betrieben wird. Der Sicherheitsgutachter muss sich davon überzeugen, dass ein einzelner Innentäter der Kontaktstelle nicht unbemerkt und unautorisiert die Zugangsdaten von al.vi und die Mailadresse für die Geräteverwaltung modifizieren kann. • Dem Anbieter des ePA-Aktensystems ist die Anforderung ebenfalls zugeordnet. Der Sicherheitsgutachter des Signaturdienstes muss sich selbst von der Umsetzung der Anforderung überzeugen. Ein Verweis auf das Sicherheitsgutachten des Anbieters ePA-Aktensystems ist nicht möglich.

Aufrechterhaltung ISMS und DSMS bei Betreibern			
GS-A_2076-01,	GS-A_2328-01,	GS-A_2329-01,	GS-A_2331-01,
GS-A_2332-01,	GS-A_2345-01,	GS-A_3737-01,	GS-A_3753-01,
GS-A_3772-01,	GS-A_4980-01,	GS-A_4981-01,	GS-A_4982-01,
GS-A_4983-01,	GS-A_4984-01,	GS-A_5551,	GS-A_5626

- Es ist darzustellen, wie der Zulassungsnehmer sicherstellt, dass die Anforderungen an das ISMS/DSMS auch in den Anteilen kontinuierlich sichergestellt wird, die von einem BTR betrieben werden. Gibt es Kontrollprozesse des ZN beim BTR? Wie erfolgen Meldungen vom BTR an den ZN (z.B. bei Vorfällen)?